Le nouvel épouvantail de la fraude bancaire s'appelle ATS

L'année 2012 s'est ouverte sur une recrudescence généralisée **des attaques informatiques**. La naissance de nouvelles conceptions du cyberactivisme n'a pas épargné les banques et autres organes financiers, ancrés dans le collimateur d'une menace émergente : les ATS.

Derrière cet acronyme se cache l'un des paradoxes de la lutte contre les fraudes bancaires en ligne : les systèmes de transfert automatique (Automatic Transfer Systems). Trend Micro s'est penché sur la question et en a conclu que les pirates parviennent désormais à déjouer les obstacles dressés à leur encontre, retournant à leur avantage les nombreuses techniques de sécurisation des transactions financières. La sophistication et l'automatisation des méthodes d'offensive ont joué un rôle crucial dans ce renouveau.

La conception originelle de la fraude bancaire impliquait des malwares (historiquement, SpyEye et ZeuS) qui exploitaient des fichiers WebInject transmis au préalable sur une machine ciblée pour injecter du code Java et HTML dans les navigateurs web, afin qu'ils affichent de fausses fenêtres de connexion par lesquelles la victime était invitée à entrer ses identifiants.

L'ennemi public numéro un : ATS

Le principe a peu ou prou perduré, mais le fichier WebInject standard s'est complexifié. Il inclut désormais des instructions d'appel à des serveurs distants auxquels sont directement délivrées les informations dérobées et des rapports détaillés de chaque opération de débit sur le compte visé. C'est en cette spontanéité que les ATS introduisent une menace supplémentaire : les noms et mots de passe volés sont immédiatement réutilisés pour procéder à des transactions incognito.

Le transfert de fonds s'effectue en cinq secondes et les preuves sont immédiatement masquées aux yeux de la victime, remplacées par de fausses informations. D'après Trend Micro, le taux d'échec reste non négligeable, mais l'on a déjà vu des sommes de 5000 à 13 000 euros disparaître dans les limbes de la Toile. La plupart des attaques proviendraient d'Europe de l'Est. Elles toucheraient essentiellement l'Allemagne, l'Italie le Royaume-Uni et dans une moindre mesure, les États-Unis.

Il est né autour des ATS un véritable marché noir. Pour s'en faire coder un sur mesure, qui puisse notamment contourner des vérifications par code confidentiel ou envoi de SMS, certains sont prêts à mettre le prix. Une solution a priori : prendre le problème à la racine et garder un œil attentif sur les principaux vecteurs d'infection que sont le phishing et les sites malveillants.